Ricardo A. Vittoni - FSS

Nápoles 3139 - C1431DEA - Cdad. de Buenos Aires - Cel. (11) 15 4416-8977 - ravittoni@gmail.com

SISTEMAS DE SEGURIDAD PARA DETECCIÓN DE MEZCLA EXPLOSIVA Y DETECCIÓN Y EXTINCIÓN DE FUEGO (SISTEMAS F&G)

SAFETY NOTE SN - 4021

FUNCIONES INSTRUMENTADAS DE SEGURIDAD PARA SISTEMAS F&G

1. Diseño Conceptual de un Sistema F&G

A fin de implementar el Sistema Seguro de Defensa Contra Incendio con Monitoreo de Mezcla Explosiva de Gas, Detección de Fuego y Disparo de Agente de Extinción (Sistema F&G), que permita prevenir explosiones, así como evitar, o reducir al mínimo posible, los daños derivados de un incendio, en Plantas de Almacenamiento, Tratamiento y/o Despacho de Gas, deberán seguirse, entre otras, las Normas prescriptivas y de performance de seguridad que se detallan a continuación:

IEC 61508	Funtional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
IEC 60079	Electrical Apparatus for Explosive Gas Atmospheres
ISA S84	Application of Safety Instrumented Systems for the Process Industries
NFPA 58	Standard for the Storage and Handling of Liquified Petroleum Gases (LPG).
NFPA 59	Standard for the Storage and Handing of LPG at Utility Gas Plant.
NFPA 59A	Standard for the Production, Storage and Handling of Liquide Natural Gas (LNG).
NFPA 69	Explosion Prevention Systems.
NFPA 70	National Electrical Code (NEC).
NFPA 72	National Fire Alarm Code

En una Planta donde se tratan, almacenan y cargan gases de pétróleo (GLP), **se deberá dar prioridad a la detección temprana y segura de niveles peligrosos de gas en el aire** (mezclas

explosivas), ya que **los eventos que presentan el mayor riesgo son las explosiones destructivas** (ver documento "Fire Protection and Gas Explosion Prevention on LPG Storage & Handling Plants" en http://infodacs.icubo.org/downloads).

> *El riesgo de una explosión destructiva se calcula, en forma simplificada, como el producto entre la probabilidad (o frecuencia) de que se produzca la explosión destructiva y la magnitud del daño (o consecuencia) que pudiera ocasionar dicha explosión (daño severo o muerte de personas presentes en el área de la explosión, valor del equipamiento destruído, lucro cesante del proceso afectado, etc.), en caso de no implementarse un Sistema de Seguridad.*

Los incendios son otra causa de destrucción de este tipo de instalaciones (y los responsables, muchas veces, de la producción de explosiones destructivas), razón por la cual también **deberá darse prioridad al aviso manual y a la detección automática de la presencia de fuego**.

No son menos importantes las acciones que el Sistema F&G deberá ejecutar ante la detección de la presencia de fuego y/o de mezclas explosivas de gas.
Estas acciones se refieren a la **desenergización de válvulas de shut-down (ESDV) y blow-down (BDV)**, así como a la **energización de válvulas diluvio (DV) y válvulas de descarga de espuma (FDV)**.

A fin de reducir el nivel de riesgo y así evitar la destrucción parcial o total de este tipo de instalaciones, **deberá proveerse un Sistema F&G de Alta Integridad que provea Funciones Instrumentadas de Seguridad (SIF), cuyo Nivel SIL sea tal que se garantice que cualquier fuga de gas sea controlada y que todo incendio sea apagado** (ver "SIF de shut-down por fuga de gas" y "SIF de extinción" más adelante).

Estas SIF deberán utilizar Detectores de Mezcla Explosiva, Detectores de Fuego, Avisadores Manuales de Incendio, secuencias lógicas dentro del Safety Logic Solver del F&G y Válvulas de Shut-Down, Blow-down, Diluvio y/o Espuma, independientes por cada "zona de fuego" y/o sector de la Planta.

El Nivel de Integridad Segura (SIL) de cada una de esas Funciones de Seguridad (SIF) **dependerá del nivel de riesgo tolerable establecido por el Usuario y del nivel de riesgo inherente de la instalación** (ver documento "Sistemas de Protección Segura para procesos Industriales" en http://infodacs.icubo.org/downloads).

El **Nivel de Riesgo Tolerable será definido por el Usuario** como la PFD_{avg} (Probaility of Failure on Demand promedio) o el SIL_{avg} (SIL promedio) de las SIF que deberá proveer el Sistema de Seguridad F&G, **basando esa definición en un Análisis de Riesgo preliminar** (HAZAN, FTA, LOPA, etc.).

> *El Nivel SIL define un rango de protección que va desde un valor mínimo a un valor máximo de Probabilidad de Falla en Demanda (PFD).*
> *Para el Nivel SIL 2, por ejemplo, la PFD debe ser menor que 1E-2 y mayor que 1E-3, mientras que para SIL 3 la PFD oscila entre 1E-3 y 1E-4 (cuando nos refiramos en este documento a "Nivel SIL 2/SIL 3", esto significará que las SIF de referencia requerirán Niveles de PFD cuyo valor estará en el orden de 1E-3).*

El Usuario deberá definir, además, el valor admisible de la PFS_{avg} (Probaility of Failure Safe promedio), **basando su definición en el nivel de lucro cesante admitido para la operación de la Planta**.

> *El **Sistema F&G accionará ante la mínima sospecha de situación de peligro, deteniendo el proceso y/o disparando los agentes de extinción, incluso cuando se trate de una "falsa alarma"**. Si así no lo hiciera, no sería un Sistema de Protección Segura.*
>
> *A este "disparo" (trip) por falsa alarma se lo conoce como "falla espuria o segura" (spurious o nuisance o safe trip) y su probabilidad de ocurrencia (PFS) se define como la cantidad de fallas seguras que el sistema puede producir en un determinado período de tiempo.*
> *Estas "fallas seguras" no producen daño a las personas, a la propiedad o al medio ambiente, pero **ocasionan importantes lucros cesantes**.*

El lucro cesante se deriva generalmente del hecho que, luego de una parada del proceso, se requieren varias horas (y a veces días) para rearrancar el mismo.

Una vez definidos por el Usuario los valores de la PFD_{avg} y de la PFS_{avg}, se diseñará el Sistema F&G de forma tal que cada SIF se ejecute dentro de los parámetros apropiados.
Una consideración muy importante a tener en cuenta en la implementación del Sistema F&G, está relacionada con le **disparo seguro de las válvulas diluvio y de descarga de espuma** (DV y FDV).

*Estas válvulas accionan cuando se las energiza, es decir, **se les debe dar tensión para que produzcan el disparo del agente de extinción**. A este tipo de disparo se lo conoce como **energize-to-trip**.*

Es decir, durante la ejecución de las "SIF de extinción" (ver más adelante), **deberá garantizarse la alimentación de las válvulas DV y FDV, con un nivel de tolerancia a fallas que dependerá del nivel SIL** de la "SIF de extinción" correspondiente.

*El "nivel de tolerancia a fallas" es **la cantidad de veces que el Sistema podrá fallar** manteniendo la garantía de integridad de la protección.*

*En **un Sistema con Nivel de Tolerancia "0"**, una "SIF de extinción" (energize-to-trip) **podrá fallar, dejando sin protección a la Planta**, cuando falle el único "canal" de disparo (entendiendo por "canal" al conjunto <detector> <módulo de entrada> <CPU del Logic Solver> <módulo de salida> <solenoide> <válvula>), o cuando falle la tensión de alimentación.*
A estos sistemas se los conoce como Sistemas en Votación 1oo1 ó Sistemas Simplex.

*Estos Sistemas pueden ser aptos para funciones de-energize-to-trip de Nivel SIL 2, pero **cuando la función deba garantizar la alimentación de la salida, el valor de integridad que provee esta arquitectura no es suficiente**.*

*En un **Sistema con Nivel de Tolerancia "1"**, un canal de disparo de la función SIF energize-to-trip podrá fallar, pero **un segundo canal "en paralelo" protegerá la Planta**.*
Estos Sistemas utilizan dos canales de disparo para cada SIF (dos detectores, dos módulos de entrada, dos CPU en el Logic Solver, dos módulos de salida, dos válvulas), así como doble fuente de alimentación.
*A fin de evitar que la falla del segundo canal pudiera dejar a la Planta sin protección, **la primer falla deberá ser detectada inmediatamente e indicada como alarma** para que pueda ser reparada con la menor demora posible.*
A estos sistemas se los conoce como Sistemas en Votación 1oo2 o Sistemas Dúplex.

Para Sistemas F&G de Nivel SIL 2 pudiera ser suficiente lan utilización de Sistemas Duplex (ya que, como se dijo, los Sistemas Simplex no son aptos para este tipo de aplicaciones).

Sin embargo, **cuando un Sistema F&G Duplex de Nivel SIL 2 tenga un canal en falla, el tiempo de reparación será crítico** y, una vez transcurrido éste, **la planta deberá ser enviada a condición segura de shut-down hasta que el Sistema F&G sea reparado**.

Para que un **Sistema F&G de Nivel SIL 2 permanezca siempre activo**, aún con un canal en falla, **la configuración mínima requerida es la que utiliza votación 2oo3** (Sistema Triplex).
Un Sistema Triplex será apto también para **Sistemas F&G de Nivel SIL 3**.

*Un Sistema en Votación 2oo3 o Sistema Triplex**, es un Sistema con Nivel de Tolerancia "2"**, es decir, que si un canal de disparo energize-to-trip de la SIF falla, **existen otros dos canales "en paralelo" para proteger la Planta**.*
Estos Sistemas utilizan, para cada SIF energize-to-trip, tres detectores, tres módulos de entrada, tres CPU en el Logic Solver, tres módulos de salida, tres válvulas y tres fuentes de alimentación (otras configuraciones usuales como dos válvulas con doble solenoide y fuentes de alimentación con redundancia N+1 son equivalentes).

*Cuando se produce **una falla en uno de los canales, ésta es detectada inmediatamente e indicada como alarma** para que pueda ser reparada. Los otros dos canales activos, con capacidad de diagnóstico, **continúan funcionando como un Sistema Duplex**.*

***El Sistema F&G con arquitectura Triplex funciona sin restricción de tiempo, aún con un canal en falla,** es decir, **sin necesidad de hacer un shut-down de la Planta**.*

1.1 Programmable Electronic Safety Controller (PESC)

El eslabón principal en la cadena de seguridad de las "SIF de shut-down por fuga de gas" y "SIF de extinción" (ver más adelante), responsable además de la ejecución de otras SIF ("SIF de despresurización", "SIF de enfriamiento de tanques", etc., no analizadas en el presente documento), es el Safety Logic Solver o **Programmable Electronic Safety-related Controller** (PESC), como lo define la Norma IEC 61508.

*El PESC se encarga de ejecutar todas las **secuencias lógicas seguras necesarias para garantizar la integridad de la Planta**. Estas secuencias lógicas están compuestas por la ejecución simple o combinada de varias SIF, de distinto Nivel SIL.*
*Según la Norma IEC 61508, **el PESC debe estar certificado por un organismo de verificación independiente** (como TÜV o FM) **para aplicaciones donde se requiera ejecutar Funciones de Seguridad de Niveles SIL 1, SIL 2 o SIL 3.***

***Los PESC se diferencian de los PLC, fundamentalmente, por su Alta Cobertura de Diagnóstico** y se clasifican, según su arquitectura, en Controladores **1oo1D** (Simplex), **1oo2D** (Dúplex) y **2oo3D** (Tríplex) o **TMR** (Triple Modular Redundancy) .*

Para su utilización en Sistemas F&G, **el PESC deberá estar homologado y Certificado según la Norma IEC 61508, ser del tipo FAILSAFE / FAULT TOLERANT y ser apto para ejecutar SIF de-energize-to-trip y energize-to-trip** (para shut-down y disparo de extinción, respectivamente).
Además, **el PESC deberá estar ensayado y Certificado según NFPA72**.

Es decir, en las SIF que ejecutará el PESC ***deberán estar garantizados el Nivel SIL y la tolerancia a fallas en todas sus partes de hardware*** *(CPU y módulos del PESC, dispositivos de campo),* ***en su instalación*** *(conexiones a dispositivos de campo debidamente implementadas)* ***y en su software de aplicación, observando estrictamente las Normas prescriptivas NFPA 72*** *como así también las* ***Normas de performance IEC 61508, IEC 61511*** *e* ***ISA S84****.*

La Norma NFPA 72 ***exige el monitoreo de línea, tanto para señales de entrada como de salida****, de forma tal que el Sistema F&G pueda indicar y actuar aún bajo condiciones de alarma como* ***cables cortados o a tierra, bobinas cortadas****, etc.*

Además de las consideraciones hechas en el punto 1, **la utilización de un PESC con arquitectura TMR resultará la opción más conveniente** si se tiene en cuenta que:

- **Los PESC TMR garantizan la separación de ejecución entre las SIF**, de forma tal que, por ejemplo, una SIF de prevención de-energize-to-trip de Nivel SIL 2 ejecutada por un canal, podrá ser considerada una "capa independiente" de otra SIF energize-to-trip de Nivel SIL 3 ejecutada en otro canal del Sistema TMR.
  Estas "capas de protección independientes" (IPL, Independent Protection Layers), brindan un mayor nivel de protección de acuerdo con el modelo LOPA ("Layers of Protection Analysis", AIChE-CCPS).

- **Los PESC TMR tienen procesadores muy poderosos**, lo cual garantiza tiempos de ejecución muy cortos y, por lo tanto, una gran cantidad de SIF en ejecución simultánea.

- **La densidad de los módulos de entrada/salida en los PESC TMR es muy alta** (más de 30 entradas analógicas por módulo), lo cual reduce el cableado y el espacio total ocupado por el Sistema, así como el costo por unidad de entrada / salida.

2. Funciones Instrumentadas de Seguridad (SIF)

2.1 SIF de shut-down por fuga de gas

Se indican a continuación las arquitecturas típicas para la ejecución de "SIF de shut-down por fuga de gas", de Nivel SIL 2 (valor promedio en la mayoría de los Procesos Industriales), **en función del nivel de disponibilidad** requerido para el Sistema.
Se considera el uso de Detectores de Gas con salida analógica. No se consideran en el ejemplo señales de realimentación y/o alarma como, por ejemplo, la de detectores POC (Proof of Closure) de las válvulas ESDV, las señales de "detector en falla", etc.

a- **Sistema Simplex - Disponibilidad BAJA** (por poseer un solo canal, una falla iniciará un shut-down de Planta).

- Dos Detectores de Mezcla Explosiva (votación 1oo2 en el software)
- Dos entradas analógicas en el PESC (una por cada Detector), del tipo 1oo1D
- Procesador 1oo1D
- Dos salidas digitales en el PESC del tipo 1oo1D (votación 1oo2 en el software)
- Dos válvulas ESDV montadas "en serie", con solenoides de disparo por corte de tensión (de-energize-to-trip)

b- **Sistema Duplex - Disponibilidad MEDIA** (una falla detendrá el Proceso cuando transcurra el tiempo crítico)

- Tres Detectores de Mezcla Explosiva (votación 2oo3 en el software)
- Tres entradas analógicas en el PESC (una por cada Detector), del tipo 1oo1D
- Procesador 1oo2D
- Dos salidas digitales en el PESC del tipo 1oo2D (votación 1oo2 en el software)
- Dos válvulas ESDV montadas "en serie", con solenoides de disparo por corte de tensión (de-energize-to-trip)

c- **Sistema Triplex - Disponibilidad ALTA** (una falla nunca detendrá el Proceso)

- Tres Detectores de Mezcla Explosiva (votación 2oo3 en el software)
- Tres entradas analógicas en el PESC (una por cada Detector), del tipo 1oo2D
- Procesador TMR
- Dos salidas digitales en el PESC del tipo TMR (votación 1oo2 en el software)
- Dos válvulas ESDV montadas "en serie", con solenoides de disparo por corte de tensión (de-energize-to-trip)

2.1.1 Detectores de Mezcla Explosiva

El primer eslabón en la cadena de seguridad de la "SIF de shut-down por fuga de gas" lo constituyen los Detectores de Mezcla Explosiva.
Es muy importante elegir la tecnología utilizada para la detección de Mezclas Explosivas teniendo en cuenta el Ciclo de Vida de la IEC 61508.

Es decir, deberán seleccionarse, siempre que sea posible, **detectores de gas del tipo FAILSAFE con Alta Cobertura de Diagnóstico libres de mantenimiento** (o que requieran mantenimiento con una frecuencia no menor a un año).
Sacando casos de excepción, donde la detección puede ser solamente del tipo catalítico o electrolítico (generalmente gases explosivos sin contenido de Carbono), se dará preferencia a la utilización de **Detectores de Absorción IR** (Infra-Roja).

> *En éstos, un emisor de doble longitud de onda (dual beam), envía, a través del aire, un "rayo" de luz infra-roja hasta un receptor ubicado a cierta distancia.*
> *La presencia de una "nube" de mezcla explosiva en el camino del "rayo" será detectada por la absorsión de la emisión en una sóla de las longitudes de onda, nivel de absorción que, por comparación con la señal "no absorbida", indicará el Nivel de Explosividad (%LEL) de la mezcla* (ver documento "Fire Protection and Gas Explosion Prevention on LPG Storage & Handling Plants" en http://infodacs.icubo.org/downloads).

Estos detectores se obtienen en versiones del tipo "detector puntual" (en los cuales emisor y receptor están separados sólo unos centímetros y tienen un radio de detección de aproximadamente 4 a 5 mts), y los del tipo "open path" (en los cuales el emisor y el receptor pueden estar separados hasta más de 100 mts, detectando fugas de gas en grandes áreas).

Cualquiera sea el tipo elegido, la cantidad de detectores a utilizar, así como la arquitectura de votación a implementar, estará relacionada con el Nivel SIL de la "SIF de shut-down por fuga de gas".
El siguiente cuadro es indicativo y su utilización deberá ser verificada en función del "rango de fallas peligrosas" (FRD, Failure Rate Dangerous), determinado por el fabricante de cada detector.

Detector Tipo	Votación SIL 1	Votación SIL 2	Votación SIL 3	Apto p/modo
Catalítico	1oo1	1oo2	-	FAILSAFE
IR	1oo1	1oo1 ó 1oo2	1oo2	FAILSAFE
IR	1oo2	2oo3	2oo3	FAULT TOLERANT

2.1.2 Válvulas de shut-down

El eslabón final en la cadena de seguridad de la "SIF de shut-down por fuga de gas" y quizá el más importante desde el momento en que es el que efectivamente realiza el corte de gas lo constituyen las válvulas de shut-down (ESDV, Emergency Shut-Down Valve) y blow-down (BDV).

Estas **válvulas deben estar aprobadas por Organismos Independientes** (por ejemplo, FM o TÜV), **para su uso específico**.

*El corte de combustible según NFPA **debe realizarse utilizando dos válvulas de shutt-down "en serie"**.*
*Para aplicaciones de Nivel SIL 2 o SIL 3, además, los cierres deben ser de nivel de hermeticidad garantizado, **leakage Class VI** según ANSI/FCI 70-2, de larga vida útil, dado el bajo nivel de prueba manual en este tipo de instalaciones (generalmente no menos de una*

vez cada 12 meses), para sostener la garantía de integridad según los pasos del Safety Life Cycle indicado por las IEC 61508.

Es imprescindible que las válvulas ESDV sean FAIL CLOSED, para que ante cualquier falla cierren el paso de gas, así como **las válvulas BDV deben ser FAIL OPEN**, de forma tal que se asegure la conexión a la línea de depresurización (o al "flare", cuando sea necesario), ante una falla.

La cantidad y tipo de válvulas a utilizar, así como la arquitectura de votación a implementar, estará relacionada con el Nivel SIL de la "SIF de shut-down por fuga de gas".
El siguiente cuadro es indicativo y su utilización deberá ser verificada en función del "rango de fallas peligrosas" (FRD, Failure Rate Dangerous), determinado por el fabricante de cada válvula.

Válvula Tipo	Votación SIL 1	Votación SIL 2	Votación SIL 3	Funcionamiento modo
ESDV, BDV	1oo1	1oo2 ó 1oo1+PST	1oo2 (+PST)	FAILSAFE

En el caso en que, por alguna razón, no se puedan utilizar válvulas ESDV o BDV múltiples, se deberán implementar técnicas de "prueba de cierre parcial" (PST, Partial Stroke Testing), para garantizar el Nivel SIL de la función de shut-down correspondiente.

2.2 SIF de extinción

Se indican a continuación las arquitecturas típicas para la ejecución de "SIF de extinción", de Nivel SIL 2 (valor promedio en la mayoría de los Procesos Industriales), en función del **nivel de disponibilidad** requerido para el Sistema.
Se analizan las SIF relacionadas con Detectores de Fuego con salida analógica (no se consideran en el ejemplo señales de realimentación y/o alarma como, por ejemplo, las señales de "detector en falla").
Las SIF relacionadas con Avisadores de Incendio en votación "NooM" son más complejas de analizar y no se detallan en este momento.

Tampoco se indican en el ejemplo las salidas digitales para iniciar el disparo remoto de “SIF de shut-down” (en caso que se utilizara un PESC independiente para esas funciones).

a- **Sistema Simplex - Disponibilidad BAJA**

No se admitirá este tipo de configuración, ya que **una falla podrá hacer que no se extinga el incendio**.

b- **Sistema Duplex - Disponibilidad MEDIA** (una falla podrá hacer que se genere un shut-down de Planta y/o que ésta se inunde con agua y/o espuma).

- Tres Detectores de Fuego por zona (votación 2oo3 en el software)
- Tres entradas analógicas en el PESC (una por cada Detector), del tipo 1oo2D
- Procesador 1oo2D
- Dos salidas digitales en el PESC del tipo 1oo2D (votación 1oo2 en el software)
- Dos válvulas DV o FDV montadas “en paralelo”, con solenoides de disparo por alimentación de tensión (energize-to-trip)

c- **Sistema Triplex - Disponibilidad ALTA** (una falla nunca detendrá el Proceso y nunca inundará la Planta)

- Tres Detectores de Fuego por zona (votación 2oo3 en el software)
- Tres entradas analógicas en el PESC (una por cada Detector), del tipo 1oo2D
- Procesador TMR
- Dos salidas digitales en el PESC del tipo TMR (votación 1oo2 en el software)
- Dos válvulas DV o FDV montadas “en paralelo”, con solenoides de disparo por alimentación de tensión (energize-to-trip)

2.2.1 Detectores de Fuego

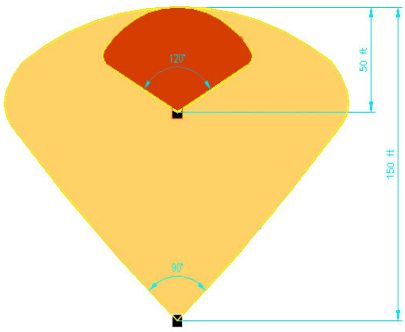
El primer eslabón en la cadena de seguridad de la "SIF de extinción" lo constituyen los Detectores de Fuego.
Es muy importante elegir la tecnología utilizada para la detección de Fuego teniendo en cuenta el Ciclo de Vida de la IEC 61508.
Es decir, deberán seleccionarse **detectores de Fuego del tipo FAILSAFE con Alta Cobertura de Diagnóstico**.

Sacando casos de excepción donde, por el tipo de llama, la detección pueda realizarse solamente con detectores del tipo UV/IR (llamas de gases con alto contenido de Hidrógeno), **se dará preferencia a la utilización de Detectores IR3** (detección de radiación Infra-Roja de Triple Banda).

Se deberá considerar, además, que **un Detector IR3 es mucho más sensible** que un Detector UV/IR y, a la vez, **totalmente inmune a todo tipo de falsas radiaciones** (lámparas halógenas, arcos de soldadura, etc.), a los que el UV/IR es sensible.

> *Estas "falsas radiaciones" son una fuente bastante frecuente de disparos espurios en los sistemas de extinción que utilizan detectores UV/IR. Como se dijo anteriormente, estos disparos espurios le generan al Usuario pérdidas por lucro cesante importantes (a menos que por cada zona se dispongan tres detectores en votación 2oo3 para descubrir la falsa alarma).*

> *Cabe hacer notar además que, como indica el gráfico, el cono de visión de los detectores IR3 es muchísimo más grande que el de los detectores UV/IR, razón por la cual, la utilización de los primeros podrá reducir notablemente la cantidad de detectores a implementar.*
> *Los detectores UV/IR suelen tener un cono de visión de 120 grados con un alcance de 15 metros, mientras que los*



detectores IR3 tienen un cono de visión *de 90 grados, pero* ***con un alcance de 60 mts****.*

Cualquiera sea el tipo elegido, la cantidad de detectores a utilizar, así como la arquitectura de votación a implementar, estará relacionada con el Nivel SIL de la "SIF de extinción".
El siguiente cuadro es indicativo y su utilización deberá ser verificada en función del "rango de fallas peligrosas" (FRD, Failure Rate Dangerous), determinado por el fabricante de cada detector y de la probabilidad de fallas espurias del mismo.

Detector Tipo	Votación SIL 1	Votación SIL 2	Votación SIL 3	Apto p/modo
UV/IR	1oo1	1oo2	1oo2	FAILSAFE
UV/IR	1oo2	2oo3	2oo3	FAULT TOLERANT
IR3	1oo1	1oo1 ó 1oo2	1oo2	FAILSAFE
IR3	1oo2	1oo2 ó 2oo3	2oo3	FAULT TOLERANT

2.2.2 Válvulas de Diluvio y de Espuma

Las válvulas diluvio (DV) y las de descarga de espuma (FDV) son el último eslabón que garantiza la efectividad de la "SIF de extinción", **deben estar aprobadas por Organismos Independientes** (por ejemplo, FM) **para su uso específico**.

Como **se deberá evitar que se inunde la Planta de agua o de espuma**, ante una falla de alimentación, **se utilizarán válvulas FAIL CLOSED.**

Sin embargo, estas válvulas **deberán ser conectadas "en paralelo" a fin de garantizar la salida del agente de extinción** cuando así lo requiera la SIF correspondiente, energizando las salidas apropiadas en el PESC, que **deberá garantizar la alimentación de independiente de los solenoides de dichas válvulas** aún en caso de una falta de tensión, por medio de la utilización de alimentación segura (UPS redundantes).
Además se deberá monitorear permanentemente la continuidad de los solenoides de actuación de las válvulas DV y FDV, a fin de prevenir una falla en el momento de su actuación.

La cantidad y tipo de válvulas a utilizar, así como la arquitectura de votación a implementar, estará relacionada con el Nivel SIL de la "SIF de extinción".
El siguiente cuadro es indicativo y su utilización deberá ser verificada en función del "rango de fallas peligrosas" (FRD, Failure Rate Dangerous), determinado por el fabricante de cada válvula.

Válvula Tipo	Votación SIL 1	Votación SIL 2	Votación SIL 3	Funcionamiento modo
DV, FDV	1oo2	1oo2 ó 2oo3	2oo3	FAILSAFE / FAULT TOLERANT (*)

(*) Como se explicó más arriba, las válvulas deben ser FAILSAFE (FAIL CLOSED) y el accionamiento, por parte del PESC, FAULT TOLERANT.

3. Consideraciones finales

3.1 Diseño Conceptual

Siguiendo los lineamientos establecidos por las Normas IEC 61508 e IEC 61511 para el Ciclo de Vida, el Diseño Conceptual del Sistema F&G considerará que:

- Cuando se trate de un Nivel SIL_{avg} = 2 existirán SIF de niveles SIL 1, SIL 2 **y SIL 3**

  Estudios recientes demuestran que en Procesos en los cuales se define un SIL_{avg} 2, existen al menos un 15% de SIF de nivel SIL 3 ("Future Trends in Safety Instrumented Systems", Kirk Fontenot, SISIS 2003).

- El nivel de riesgo de las SIF de Nivel SIL 3 ó SIL 2 / SIL 3 podrá ser reducido a SIL 2 utilizando capas adicionales de protección ("Layers Of Protection Analysis", AIChE-CCPS) y/o **deberán utilizarse arquitecturas de protección SIL 3** para ejecutar dichas SIF.

- El Nivel de Protección SIL 2 **deberá ser mantenido a lo largo de todo el Ciclo de Vida** por medio de la prueba periódica, a intervalos regulares, del funcionamiento de todas las SIF.

  Durante las tareas de prueba del Sistema F&G deberán relevarse de su función los elementos bajo prueba (por ejemplo, se anularán una por una las DV y FDV para evitar la inundación de la Planta con el agente de extinción durante su ensayo). Durante la ejecución de las pruebas, el Nivel SIL deberá ser mantenido.

- Se deberá garantizar la máxima disponibilidad de la Planta, con la mínima probabilidad de disparos espurios, **reduciendo al mínimo las pérdidas por lucro cesante**.

- Se adoptará preferentemente un **Sistema Triplex de Alta Disponibilidad**.

La provisión del PESC incluirá el suministro de un terminal gráfico color que **mostrará todos los mensajes de advertencia y alarma** relacionados con cada situación anormal en la cual intervenga el Sistema de Seguridad, **así como graficará las zonas de fuego** indicando su estado en forma permanente.
Este terminal gráfico o Panel de Operador color tendrá pantalla “Touch TFT” de 10” (mínimo) y podrá ser del tipo PC o hardware dedicado. En cualquiera de los dos casos, el terminal proveerá los protocolos de comunicación apropiados (MODBUS, TCP/IP, etc.)

Como todo Sistema de Seguridad requiere de una Work Station para poder realizar las verificaciones periódicas de correcto funcionamiento del Sistema (mantenimiento anual), así como para poder realizar eventuales modificaciones y/o ampliaciones del mismo, se proveerá una PC fija (o una “Notebook” portátil), que correrá las herramientas de programación y mantenimiento del PESC.

Inclusive podrá proveerse, junto con la PC, un software de visualización (HMI/SCADA).

De esta forma, la PC podrá proveer las funciones propias del Panel de Operador pudiéndose, de esta forma, utilizar solamente la PC como único dispositivo de Visualización, Programación, Configuración y Mantenimiento del PESC y del Sistema F&G.
De esta forma, esta PC **cumplirá la doble función de Panel de Operador y Estación de Trabajo (WS) del Sistema F&G** (esta última función con restricción de acceso protegido por password), reduciendo así los costos del equipamiento y simplificando la operación del Sistema F&G.

3.2 Acerca de la instalación

Siempre que sea posible, se preferirá la conexión directa de los dispositivos de campo hasta el gabinete de la CPU del PESC, en lugar de la instalación de la CPU en Sala de Control y las unidades de entrada/salida en Campo (remotas).

> *Por tratarse de un Sistema de Alta Integridad, la conexión entre la CPU y los chassis remotos deberá realizarse por medio de una red de campo de alta integridad o "bus de seguridad", el cual deberá garantizar el mismo nivel de integridad que el resto del Sistema.*
> *La implementación de esta conexión de alta integridad se consigue instalando un "master" de comunicaciones en el chassis principal de la CPU, un "slave" de comunicaciones en el chassis remoto, y un medio físico apropiado para interconectarlos (bus de fibra óptica).*
> *Para garantizar el Nivel de Integridad requerido, tanto el scanner, como el adapter como las fibras ópticas deberán ser duplicados o triplicados (dependiendo del nivel de disponibilidad requerido.*

El Sistema F&G podrá montarse, entonces según dos variantes alternativas:

a) Instalando el gabinete que contiene al PESC en Sala de Control

En este caso, se tenderán hasta Sala de Control todos los cables de los dispositivos de Campo.

El Panel de Operador será ubicado en el mismo armario del PESC o en un pupitre de comando, y se conectará directamente, con cable mallado, a uno de los puertos de comunicación del PESC (a menos que una única PC cumpla las dos funciones, como se vió más arriba).
La Estación de Trabajo (WS) del PESC se conectará también directamente, a otro de los puertos del PESC.

b) Instalando el gabinete que contiene el PESC en Campo

En este caso, el terminal gráfico y/o la WS, ubicado(s) en la Sala de Control se conectará(n) al PESC por medio de un enlace propiado el cual dependerá de la distancia a cubrir (enlace de fibra óptica, cable coaxil, etc., con el protocolo adecuado.

Esta alternativa requerirá, muy probablemente, de la **instalación de un Sistema de Purga y Presurización** en el gabinete del PESC debido a que el área de instalación en Campo podrá ser clasificada (Zona 1 ó Zona 2 según IEC 60079).

4. Ingeniería del Sistema F&G

Tal como establece la IEC 61508 para el Ciclo de Vida del Sistema de Seguridad, **la Ingeniería del Sistema en su totalidad**, incluyendo las correspondientes a la instalación de los elementos de campo y a la instalación, programación y puesta en marcha del PESC, **debe ejecutarse de forma tal de garantizar el Nivel de Integridad SIL_{avg} y el Nivel SIL** (SIL 1, 2 ó 3) **de cada función SIF**.

4.1 Ingeniería de la Instrumentación

Tal como establece la IEC 61511**, para diseñar el Sistema F&G definitivo será necesario ejecutar un estudio cauntitativo** (HAZAN, FTA, LOPA, etc.), **a fin de verificar el Nivel de Integridad SIL 2 (promedio) especificado**, así como para **establecer todas las SIF necesarias y**

evaluar su correspondiente Nivel SIL. De esta forma se podrán definir las cantidades y tipos definitivos de los componentes de campo a utilizar.

Las exigencias actuales de seguridad obligan a un trabajo de Ingeniería de Instrumentación que diseñe cuidadosamente un eficiente esquema de operatividad y sus automatismos de protección de acuerdo con las Normas.

Esta Ingeniería deberá ser desarrollada con un alto grado de experiencia y confiabilidad por parte del Proveedor, quien suministrará los Servicios de Ingeniería requeridos, incluyendo la provisión de típicos de montaje y un listado completo de la instrumentación necesaria para cumplir con el Nivel SIL y con la disponibilidad del Sistema.

4.2 Ingeniería de Programación, Commissioning y Puesta en Marcha del PESC

Por tratarse de un Sistema de Seguridad homologado con las Normas IEC 61508, IEC 61511 e ISA S84.01, **la programación del PESC deberá seguir estrictos criterios de programación, validación y verificación de las secuencias y algoritmos lógicos correspondientes a cada SIF**, sobre todo para aquéllas de Nivel SIL 2 y SIL 3.

Para la programación de SIF de estos Niveles SIL se utilizarán preferentemente **Bloques de Programación Certificados, Programación Estructurada y se proveerá un diagrama de flujo para cada SIF**, indicando claramente las previsiones de seguridad tomadas para cada condición de falla.

El Sistema deberá proveer, además, **un listado completo de mensajes de advertencia y alarma** (los cuales serán mostrados en el Panel de Operador y/o en la WS), para cada situación en la cual intervenga el Sistema de Seguridad. El Panel de Operador y/o la WS del Sistema F&G mostrará(n) además todos los gráficos de zonas de fuego del Sistema.

La provisión del PESC incluirá el FAT (Factory Acceptance Test) en sede del fabricante del equipamiento y/o del Integrador o Proveedor del Sistema.
Asimismo deberán ser provistos junto con el Sistema, todos los servicios de Campo necesarios: OSAT (On-Site Acceptance Test), Commissioning y Puesta en Marcha.

Ricardo A. Vittoni - FSS
Functional Safety Specialist